Artificial intelligence is changing the game for cybersecurity across several industries; by providing cutting-edge security technologies. Today, several organizations are increasingly implementing AI-powered intelligent solutions & services to understand and reuse threat patterns for identifying new threats. AI technologies such as machine learning and natural language processing enable organizations to analyze massive quantities of risk data to speed response times and augment under-resourced security operations. In addition, AI is also used to analyze user behaviors, deduce a pattern, identify abnormalities or irregularities in the network, and identify cyber vulnerabilities expeditiously in organizations.

Meticulous Research®, in its latest publication on the artificial intelligence in cybersecurity market, states that **the global artificial intelligence in cybersecurity market will grow at a CAGR of 24.2% from 2022 to 2029 to reach USD 66.22 billion by 2029.** The growth of this market is driven by the increasing demand for advanced cybersecurity solutions and privacy, the growing significance of AI-based cybersecurity solutions in the banking sector, increasing frequency and complexity of cyber threats.

The lack of skilled AI professionals and the perception of AI in cybersecurity as an uncomprehensive security solution are expected to restrain the growth of this market. However, the growing need for AI-based cybersecurity solutions among small and medium-sized enterprises (SMEs) is expected to create growth opportunities for the vendors operating in this market. Furthermore, misconceptions and a lack of knowledge regarding AI in cybersecurity solutions and vulnerability issues with IoT devices are major challenges for the growth of this market.

Additionally, the incorporation of advanced technologies is an ongoing trend in this market. Although the impacts of the COVID-19 pandemic may hinder the growth of the market this year, the increasing demand for advanced cybersecurity solutions for protection against cyber threats in industry verticals is expected to enable the growth of the artificial intelligence in cybersecurity market in the coming years.

Download Free Sample Report Now @ https://www.meticulousresearch.com/download-sample-report/cp_id=5101

To provide efficient analysis, Meticulous Research® has segmented this market based on components (hardware, software, services), technology (machine learning, natural language processing, context-aware computing), by security (application security, endpoint security, cloud security, network security), applications (data loss prevention, unified threat management, encryption, identity & access management, risk & compliance management, antivirus/antimalware, intrusion detection/prevention system, distributed denial of service mitigation, security information & event management, threat intelligence, fraud detection), deployment (on-premises, cloud), industry vertical (retail, government & defense, automotive & transportation, BFSI, manufacturing, infrastructure, IT & telecommunication, healthcare, aerospace, education, energy), and geography (North America, Europe, Asia-Pacific, Latin America, and the Middle East & Africa).

Based on security, the market is segmented into application security, network security, endpoint security, and cloud security. In 2022, the network security segment is estimated to account for the largest share of the overall artificial

intelligence in cybersecurity market. The growth of this segment is attributed to an increase in the adoption of the Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD) trends, the increasing demand for advanced security services, the rising numbers of APTs, malware, and phishing attacks, and the growing need of security solutions for cloud technology. However, the cloud security segment is slated to register the highest CAGR during the forecast period due to the increasing number of security breaches and cyberattacks on cloud infrastructure, the increasing adoption of cloud servers, and the surge in demand for robust and cost-effective security services.

Based on geography, the artificial intelligence in cybersecurity market is segmented into North America, Europe, Asia-Pacific, Latin America, and the Middle East & Africa. In 2022, North America is estimated to account for the largest share of the artificial intelligence in cybersecurity market. The large market share of North America is attributed to the presence of major players in the region, increase in government initiatives towards advanced technologies, such as artificial intelligence, cloud, IoT, and increasing sophistication of cyber-attacks. However, Asia-Pacific is expected to register the highest CAGR during the forecast period. The high market growth in Asia-Pacific is attributed to the rising number of connected devices, increased privacy & security concerns, the growing awareness regarding cybersecurity among organizations, the increasing adoption of cloud-based solutions, and the rising cyber threats.

The report provides competitive intelligence in terms of financials, growth strategies, product portfolios, and geographical presence on the key players operating in the artificial intelligence in cybersecurity market, including Amazon Web Services, Inc. (U.S.), IBM Corporation (U.S.), Intel Corporation (U.S.), Microsoft Corporation (U.S.), Nvidia Corporation (U.S.), FireEye, Inc. (U.S.), Palo Alto Networks, Inc. (U.S.), Juniper Networks, Inc. (U.S.), Fortinet, Inc. (U.S.), Cisco Systems, Inc. (U.S.), Micron Technology, Inc. (U.S.), Check Point Software Technologies Ltd. (U.S.), Imperva (U.S.), McAfee LLC (U.S.), LogRhythm, Inc. (U.S.), Sophos Ltd. (U.S.), NortonLifeLock Inc. (U.S.), and Crowdstrike Holdings, Inc. (U.S.).